Method for carrying out a secure transaction, especially downloading of software, between a mobile phone equipped with a SIM card and an application server, whereby hash encryption is used to ensure the transaction is secure

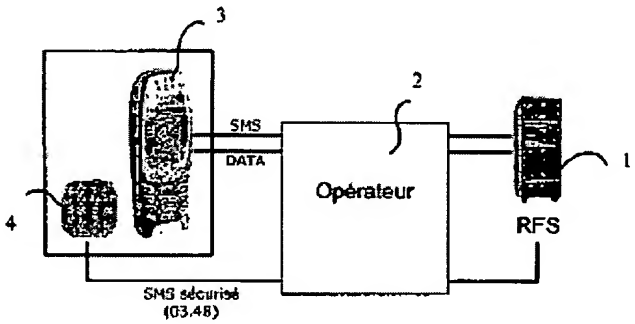
Patent number: FR2831362
Publication date: 2003-04-25
Inventor: DE BELEN PIERRE
Applicant: BABEL SOFTWARE (FR)
Classification:
- international: ***G07F7/10; H04Q7/32;*** **G07F7/10; H04Q7/32;** (IPC1-7): H04L9/32; G06F17/60; H04L9/30; H04Q7/22
- european: G07F7/10D2P; G07F7/10D4E; H04Q7/32S
Application number: FR20010013523 20011019
Priority number(s): FR20010013523 20011019

Also published as:
WO03041022 (A1)

Report a data error here

Abstract of **FR2831362**

Method has the following steps: public encryption keys are exchanged between subscriber and server; the subscriber sends a request file to the server for purchase of a downloadable application, whereby the file is sent as a message and a hash encrypted element; an order is transmitted to the subscriber from the server in the form of a signed file and a hash file; and finally transmission of the downloadable application (MIDLET) to the subscriber.



Data supplied from the ***esp@cenet*** database - Worldwide

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 831 362**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **01 13523**

(51) Int Cl[7] : **H 04 L 9/32**, H 04 L 9/30, G 06 F 17/60, H 04 Q 7/22

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 19.10.01.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 25.04.03 Bulletin 03/17.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *BABEL SOFTWARE Société par actions simplifiée* — FR.

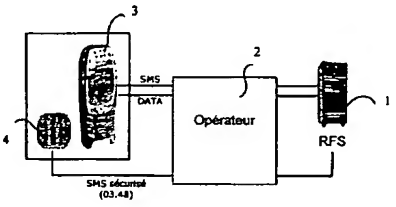
(72) **Inventeur(s) :** DE BELEN PIERRE.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** BREESE MAJEROWICZ SIMONNOT.

(54) PROCEDE DE TRANSACTION SECURISEE ENTRE UN TELEPHONE MOBILE EQUIPE D'UN MODULE D'IDENTIFICATION D'ABONNE (CARTE SIM) ET UN SERVEUR D'APPLICATION.

(57) La présente invention concerne un procédé de transaction sécurisée entre un téléphone mobile équipé d'un module d'identification d'abonné (carte SIM) et un serveur d'application, caractérisé en ce qu'il comporte une étape d'échange sécurisé des clés publiques entre le serveur et l'abonné et d'enregistrement par l'abonné de la clé publique Ks_pub du serveur, et d'enregistrement sur le serveur de la clé publique Ku_pub de l'abonné, une étape d'achat d'applications téléchargeables consistant à préparer un fichier numérique de demande sur l'équipement mobile, et à transmettre au serveur d'une part ledit fichier numérique sous forme d'un message et d'autre part de transmettre un condensat chiffré, une étape de transmission de commande par le serveur à l'abonné sous forme de fichier numérique signé et sous forme d'un condensat dudit fichier, et une étape de transmission par le serveur à l'abonné d'une application téléchargeable [MIDLET] comprenant une partie seulement codée.



FR 2 831 362 - A1

PROCEDE DE TRANSACTION SECURISEE ENTRE UN TELEPHONE MOBILE EQUIPE D'UN MODULE D'IDENTIFICATION D'ABONNE (CARTE SIM) ET UN SERVEUR D'APPLICATION

La présente invention concerne le domaine des transactions entre un serveur d'application et un équipement mobile, notamment un téléphone, équipé d'un module d'identification d'abonné, par exemple une carte SIM.

De tels équipements permettent d'échanger des données numériques sous une forme sécurisée, par exemple sous la forme de paquet de commande selon un format défini par la norme GSM 03.48.

Le but de l'invention est de proposer un procédé permettant d'assurer des échanges et transactions numériques entre un serveur d'application et un téléphone identifiés avec un haut degré de sécurité, par :

- une authentification de l'utilisateur par le serveur (paiement)
- une authentification du serveur par l'utilisateur (réception de commandes)
- une protection des droits (copyright) lors de l'exécution de MIDLET
- une certification de la MIDLET par l'intermédiaire d'une signature.

A cet effet, l'invention concerne selon son acception la plus générale un procédé de transaction sécurisé entre un téléphone mobile équipé d'un module d'identification d'abonné (carte SIM) et un serveur d'application, caractérisé en ce qu'il comporte une étape d'échange sécurisé des clés publiques entre le serveur et l'abonné et d'enregistrement par l'abonné de la clé publique Ks_pub du serveur, et d'enregistrement sur le serveur de la clé publique Ku_pub de l'abonné, une étape d'achat d'applications téléchargeables

consistant à préparer un fichier numérique de demande sur l'équipement mobile, et à transmettre au serveur d'une part ledit fichier numérique sous forme d'un message et d'autre part de transmettre un condensat chiffré, une étape de transmission de commande par le serveur à l'abonné sous forme de fichier numérique signé et sous forme d'un condensat dudit fichier, et une étape de transmission par le serveur à l'abonné d'une application téléchargeable [MIDLET] comprenant une partie seulement codée.

La présente invention sera mieux comprise à la lecture de la description d'un exemple non limitatif de réalisation, faisant référence aux dessins annexés où :

- la figure 1 représente une vue générale de l'architecture du système mis en œuvre par l'invention ;
- la figure 2 représente une vue schématique de la transmission de la clé publique de l'abonné au serveur
- la figure 3 représente une vue schématique de la transmission de la clé publique du serveur à l'abonné
- La figure 4 représente une vue schématique de l'opération de paiement
- La figure 5 représente une vue schématique de l'opération de réception de commandes
- Les figures 6 et 7 représentent des vues schématiques des opérations de protection des droits
- Les figures 8 et 9 représentent des vues schématiques des opérations de vérification de la provenance et de l'intégrité des applications chargées.

L'invention met en œuvre un serveur d'application (1) comprenant un serveur de messages courts (SMS) via un réseau de télécommunication exploité par un opérateur (2). L'abonné destinataire des services fournis par le serveur d'application (2) est équipé d'un équipement mobile, par

exemple un téléphone mobile (3) équipé de façon connue par un module d'identification de l'abonné (4) sous forme de carte SIM.

L'abonné et le serveur procèdent à un échange de leurs clés publiques respectives.

Une première étape consiste à identifier l'abonné par le serveur d'application.

Pour relier, de façon certaine, un nom de client à une clé publique, on transmet au serveur la clé publique calculée par la carte grâce à un SMS sécurisé. Cette technique présente l'avantage de ne jamais faire sortir la clé publique de la carte.

Si le SMS sécurisé n'est pas utilisable, on pourra utiliser des certificats de tierce partie.

L'échange de clés s'effectue de manière aléatoire.

La figure 2 représente une vue schématique de l'opération de génération des clés publiques et privées de l'abonné. Le module d'identification de l'abonné (4) génère une bi-clé comportant :

- une clé privée Ku_priv
- une clé publique Ku-pub.

Cette génération de bi-clé est réalisée dans la carte SIM, et n'est pas transmise à l'environnement de la carte.

La clé publique Ku_pub est transmise au serveur (1) dans le paquet de commande conforme à la norme GSM 03.48, dans le champ "DATA", sous forme de message court SMS sécurisé.

Le serveur génère également un bi-clé Ks-priv, Ks_pub comme représenté en figure 3. La clé publique Ks_pub est chiffré avec la clé publique Ku_pub de l'abonné est est transmise à l'abonné sous forme de message court SMS.

Le moteur d'application JAVA JAM de l'équipement mobile déchiffre le paquet de commande et enregistre sur la

mémoire de l'équipement mobile la clé publique Ks_pub du serveur.

Le procédé comporte des opérations d'achat d'application téléchargeable [MIDLETs].

L'achat de MIDLETs doit être sécurisé. Le but est de s'assurer que c'est bien le bon client qui donne l'ordre d'acheter. On doit donc signer la demande. La demande est émise par le canal modem. En effet pour acheter des MIDLETS l'utilisateur se servira du PACKAGE MANAGER qui initialise le modem.

La figure 4 représente une vue schématique de l'opération de paiement.

La demande de l'abonné prend la forme d'un fichier numérique qui est transmis au serveur (1) par le canal MODEM.

Parallèlement, l'équipement mobile calcule un condendat (5) [HASH] qui est transmis au serveur sous une forme chiffrée par une fonction de chiffrement F(RES, Ku_priv) avec la clé privée de l'abonné.

Le serveur vérifie l'intégrité de la demande et authentifie l'émetteur de la demande par recalcul du condensat du fichier numérique reçoit sur le canal Modem et par comparaison avec le condensat déchiffré avec la clé publique Ku_publique de l'utilisateur, précédemment enregistrée.

La réception de commandes est décrite en référence à la figure 5. Les commandes sont des instructions de service émises par le serveur (1) à l'intention d'un ou de plusieurs abonnées. Il s'agit par exemple d'une commande de chargement d'une application [MIDLET] sur un équipement abonné, ou d'effacement d'un telle application. Les commandes provenant du RFS par le canal SMS doivent être signées, pour être sûr qu'une commande, 'EFFACE' par exemple, a bien été envoyée par l'opérateur.

Le serveur (1) prépare un fichier numérique correspondant à la commande et la transmet par le canal Modem ou sous forme de message court SMS à l'abonné, sous une forme signé par une fonction de signature F(Sign, Ks_pub). Il calcule par ailleurs un condensat transmis à l'abonné. La carte SIM de l'abonné procède à un test de validité et exécute la commande si le test est positif.

Les figures 6 et 7 représentent des vues schématiques des opérations de protection des droits.

Cette opération permet d'éviter qu'une application [MIDLET] ne puisse être utilisée que par la personne qui l'a achetée.

Le serveur génère une clé symétrique aléatoire lors du chargement d'un fichier. Cette clé sert à crypter certaines parties de la MIDLET.

La MIDLET est ensuite envoyée avec la clé symétrique cryptée par la clé publique du client. La clé symétrique est alors décryptée dans la carte qui stocke un couple [MIDLETID, clé symétrique]

A chaque demande d'utilisation d'une MIDLET le moteur d'application JAVA JAM demande à la carte de décrypter (en utilisant la clé symétrique) les morceaux codés. On ne code pas toute la MIDLET car la bande passante entre la mémoire vive du téléphone et la carte SIM est assez faible.

Les figures 8 et 9 représentent des vues schématiques des opérations de vérification de la provenance et de l'intégrité des applications chargées.

On doit assurer la provenance et l'intégrité de la MIDLET. La vérification de la provenance est effectuée au chargement, et la vérification de l'intégrité à chaque utilisation.

Au chargement le serveur envoie la MIDLET et sa signature.

La carte décrypte la signature et sauvegarde le résultat de la fonction de HASH en association avec une ID de la MIDLET

La carte vérifie ensuite la validité de la signature et communique le résultat à la JAM

Au chargement le serveur envoie la MIDLET et sa signature.

La carte décrypte la signature est sauvegarde le résultat de la fonction de HASH en association avec une ID de la MIDLET

La carte vérifie ensuite la validité de la signature et communique le résultat à la JAM

REVENDICATIONS

1 – Procédé de transaction sécurisée entre un téléphone mobile équipé d'un module d'identification d'abonné (carte SIM) et un serveur d'application, caractérisé en ce qu'il comporte une étape d'échange sécurisé des clés publiques entre le serveur et l'abonné et d'enregistrement par l'abonné de la clé publique Ks_pub du serveur, et d'enregistrement sur le serveur de la clé publique Ku_pub de l'abonné, une étape d'achat d'applications téléchargeables consistant à préparer un fichier numérique de demande sur l'équipement mobile, et à transmettre au serveur d'une part ledit fichier numérique sous forme d'un message et d'autre part de transmettre un condensat chiffré, une étape de transmission de commande par le serveur à l'abonné sous forme de fichier numérique signé et sous forme d'un condensat dudit fichier, et une étape de transmission par le serveur à l'abonné d'une application téléchargeable [MIDLET] comprenant une partie seulement codée.

2 - Procédé de transaction sécurisée selon la revendication 1, caractérisé en ce que l'étape d'échange sécurisé des clés publiques comporte une étape de génération par le module d'identification de l'abonné (4) d'une bi-clé comportant une clé privée Ku_priv et une clé publique Ku-pub et une opération de transmission de la clé publique Ku_pub au serveur (1) sous forme de message court sécurisé, et une opération de génération d'une bi-clé Ks-priv, Ks_pub, puis de transmission par le serveur à l'abonné de ladit clé publique Ks_pub chiffrée avec la clé publique Ku_pub de sous forme de message court.

3 - Procédé de transaction sécurisée selon la revendication 1 ou 2, caractérisé en ce que l'étape d'achat

d'application téléchargeable [MIDLETs] comporte une opération de transmission au serveur d'un fichier numérique par le canal MODEM et de calcul par l'équipement mobile émetteur de la commande d'un condendat (5) [HASH] qui est transmis au serveur sous une forme chiffrée par une fonction de chiffrement F(RES, Ku_priv) avec la clé privée de l'abonné et une opération de vérification de l'intégrité de la demande et d'authentification par l'émetteur de la demande par recalcul du condensat du fichier numérique reçoit sur le canal Modem et par comparaison avec le condensat déchiffré avec la clé publique Ku_publique de l'utilisateur, précédemment enregistrée.

4 - Procédé de transaction sécurisée selon la revendication 1, caractérisé en ce que l'étape de transmission d'une commande comporte une opération de préparation par le serveur (1) d'un fichier numérique correspondant à la commande et de transmission par le canal Modem ou sous forme de message court SMS à l'abonné, sous une forme signé par une fonction de signature F(Sign, Ks_pub) et de calcul d'un condensat transmis à l'abonné.

5 - Procédé de transaction sécurisée selon la revendication 1, caractérisé en ce que l'étape de protection des droits consiste à générer, par le serveur, d'une clé symétrique aléatoire lors du chargement d'un fichier, ladite clé servant à crypter certaines parties de la MIDLET.

6 - Procédé de transaction sécurisée selon la revendication 5, caractérisé en ce que l'application [MIDLET] est ensuite envoyée avec la clé symétrique cryptée par la clé publique du client, la clé symétrique étant ensuite décryptée dans la carte qui stocke un couple [MIDLETID, clé symétrique]

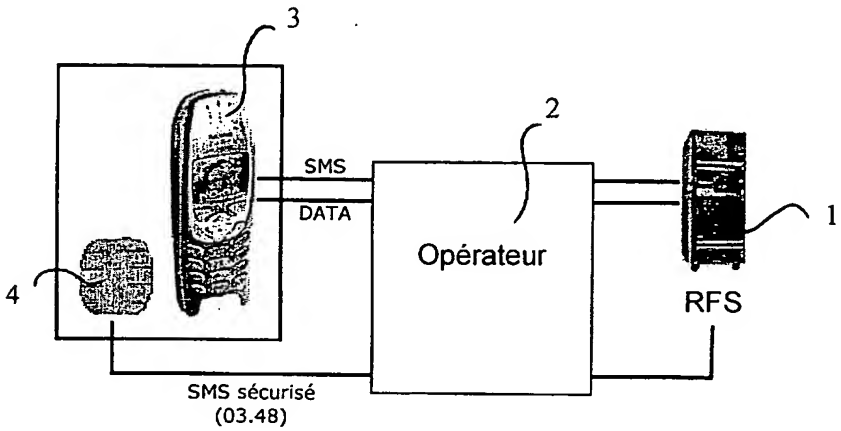
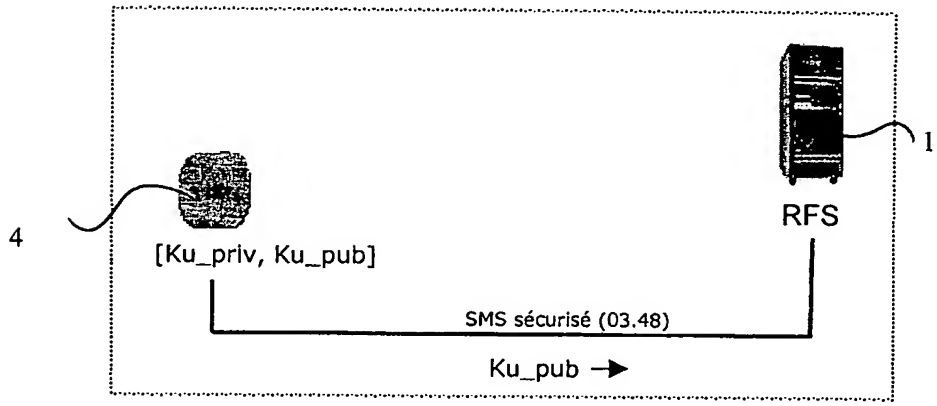
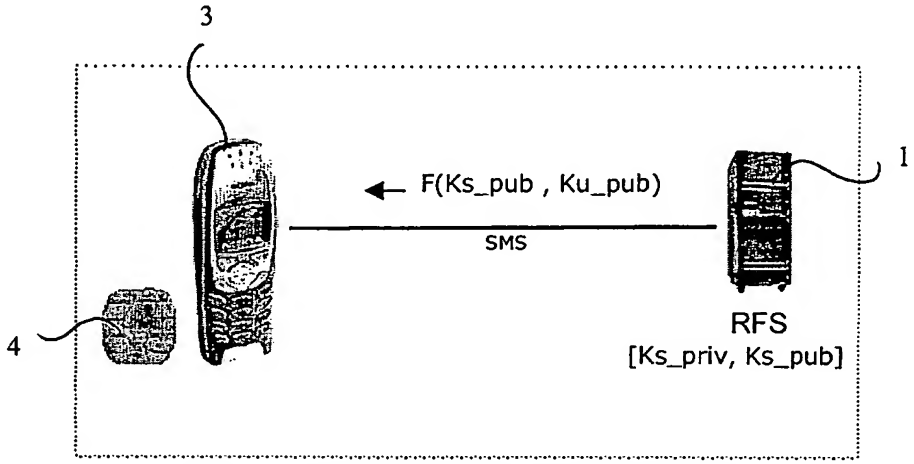


Figure 1



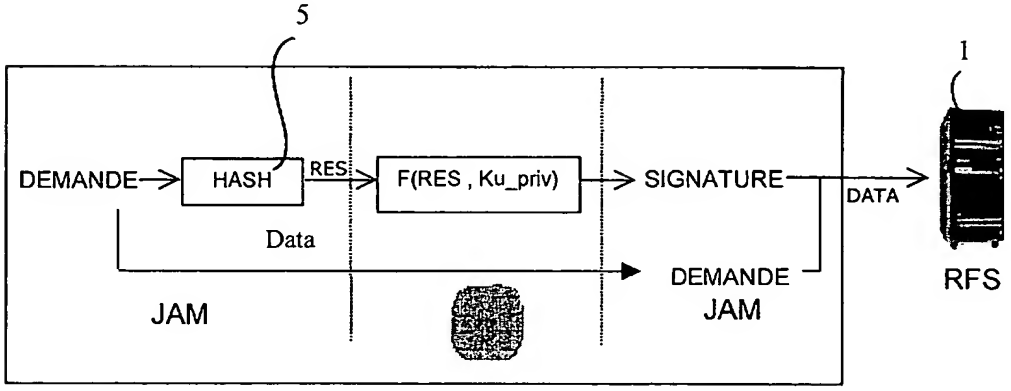
La carte génère les clés publique et privée et envoie la clé publique au RFS grâce à un SMS sécurisé

Figure 2



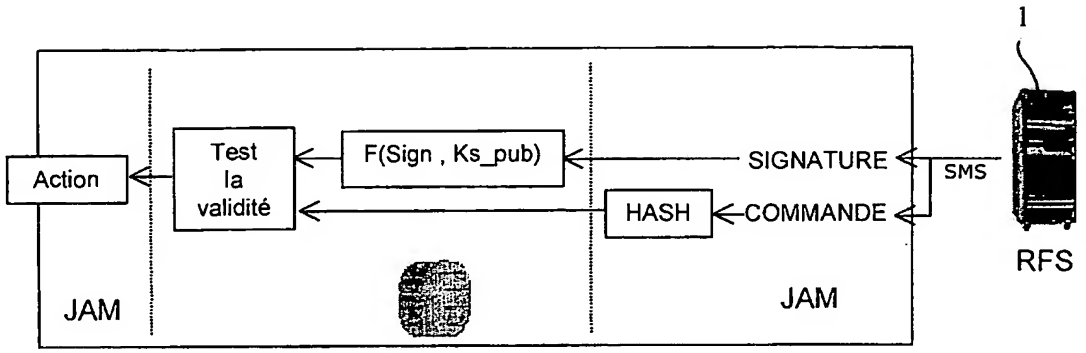
RFS crypte sa clé publique et l'envoie à la JAM du téléphone

Figure 3



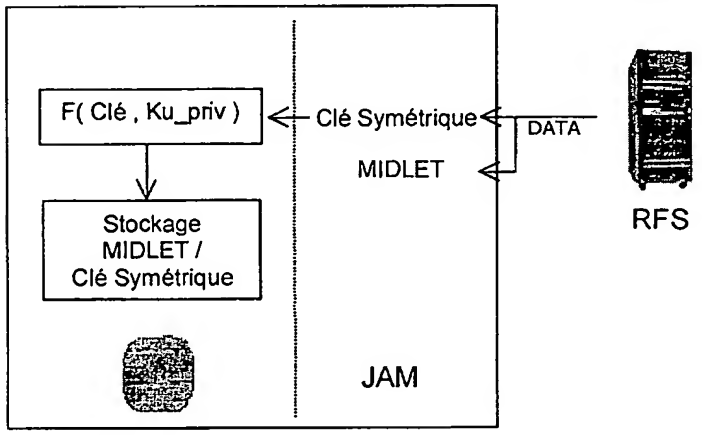
La JAM crée la demande puis génère un HASH.
Ce HASH est crypté par la carte avec la clé privée de l'utilisateur.
La demande est ensuite envoyée avec sa signature au serveur RFS

Figure 4



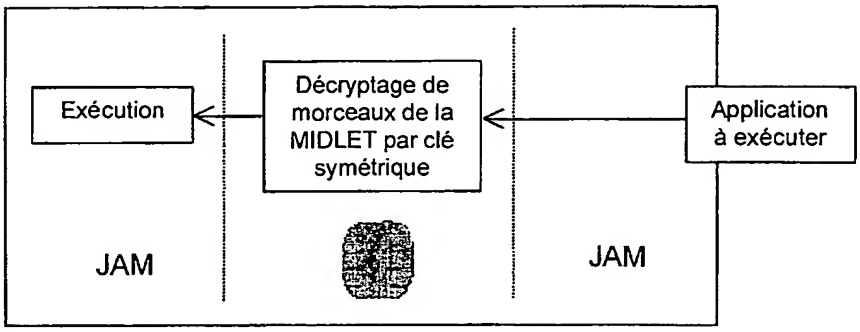
Le serveur envoie une commande signée.
La puce décrypte la clé de HASH et compare au HASH généré par la JAM.
Selon le résultat la JAM peut effectuer ou non la commande.

Figure 5



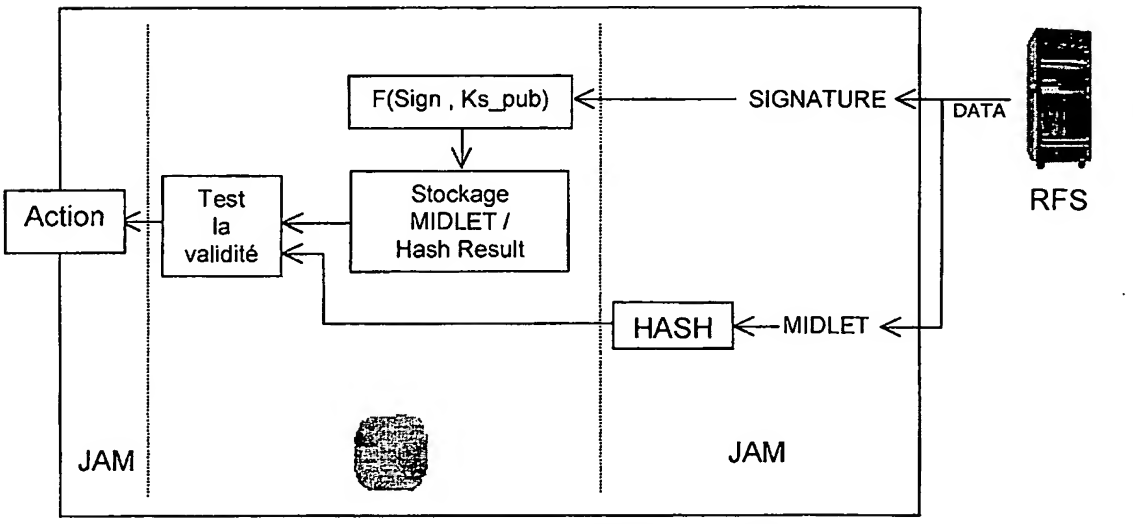
On envoie la MIDLET cryptée et la clé symétrique protégée par la clé asymétrique du client.
La carte décrypte la clé symétrique qu'elle stocke en association avec une ID de la MIDLET

Figure 6



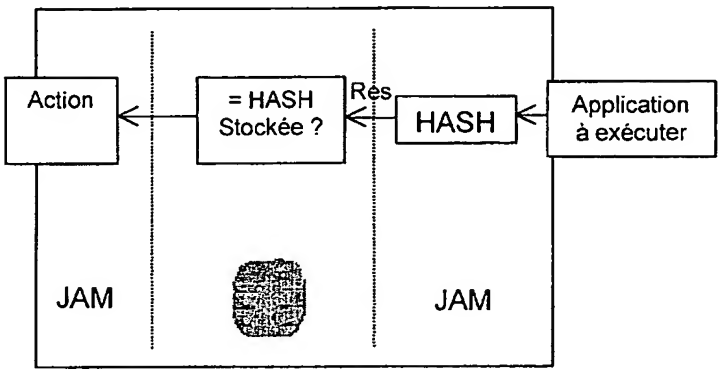
Lors d'une utilisation, la JAM demande a la carte de décrypter les parties cryptées de la MIDLET, puis elle exécute la MIDLET.

Figure 7



Au chargement le serveur envoie la MIDLET et sa signature.
La carte décrypte la signature et sauvegarde le résultat de la fonction de HASH en association avec une ID de la MIDLET
La carte vérifie ensuite la validité de la signature et communique le résultat à la JAM

Figure 8



Lors de l'utilisation de la MIDLET, la JAM calcule la fonction de HASH et demande à la carte de comparer le résultat avec la valeur stockée. Ce qui permet d'effectuer le lancement de l'application ou une autre action.

Figure 9

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2831362

N° d'enregistrement national

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

FA 613399
FR 0113523

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
Y	EP 0 910 028 A (MATSUSHITA ELECTRIC IND CO LTD) 21 avril 1999 (1999-04-21) * colonne 4, ligne 25 - ligne 43 * * colonne 81, ligne 55 - colonne 83, ligne 23 *	1-6	H04L9/32 H04L9/30 G06F17/60 H04Q7/22
Y	US 6 223 291 B1 (VOGLER DEAN H ET AL) 24 avril 2001 (2001-04-24) * figure 5 * * colonne 1, ligne 8 - ligne 15 * * colonne 2, ligne 44 - ligne 52 * * colonne 3, ligne 15 - ligne 28 * * colonne 7, ligne 27 - ligne 42 * * colonne 8, ligne 3 - ligne 5 *	1-6	
A	O'MAHONY ET AL.: "Electronic payment systems" 1997 , ARTECH HOUSE , BOSTON XP002113876 * page 19 - page 61 *	1	
			DOMAINES TECHNIQUES RECHERCHÉS (Int.Cl.7)
			G07F

Date d'achèvement de la recherche	Examinateur
2 juillet 2002	Verhoef, P

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

1

2831362

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0113523 FA 613399

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 02-07-2002
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP 0910028	A	21-04-1999	JP	10198739 A	31-07-1998
			EP	0910028 A1	21-04-1999
			US	6332133 B1	18-12-2001
			CN	1212773 A	31-03-1999
			WO	9821677 A1	22-05-1998
US 6223291	B1	24-04-2001	AU	3498600 A	16-10-2000
			CN	1345494 T	17-04-2002
			EP	1166490 A1	02-01-2002
			WO	0059149 A1	05-10-2000

EPO FORM P0465

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82